



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/781,476	02/12/2001	Bjorn Markus Jakobsson	39	9477

7590 04/21/2005

Ryan, Mason & Lewis, LLP  
90 Forest Avenue  
Locust Valley, NY 11560

EXAMINER
----------

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/781,476

Applicant(s)

JAKOBSSON, BJORN MARKUS

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 24 November 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

***DETAILED ACTION***

1. This action is responsive to communication: 24 November 2004, the original application was filed on 12 February 2001.
2. Claims 1-18 are currently pending in this application. Claims 1, 17, and 18 are independent claims.

***Response to Arguments***

3. Applicant's arguments with respect to claims 1-18 have been considered but are not persuasive.

In response to applicant's argument beginning on page 2, "Brickell does not describe the use of a "proof of correctness" to indicate "that the message is of a type that allows decryption by one more escrow authorities". The Office disagrees, Brickell clearly shows proof of correctness with an escrow authority, in the referenced patent the FIELD OF THE INVENTION states: "The present invention relates to multi-step digital signature systems. More particularly, the present invention relates to the management of the cryptographic keys used by certification authorities in multi-step digital signature systems". The term "proof of correctness" can be interpreted as 'verifying that a certifying authority is correct by presented to a higher tier certifying authority which issues a certificate, authenticating the signature' see col. 3, lines 60-65. The certifying authorities verify that the 'message is a type that allow decryption by one or more escrow authorities' is inherent with the communication described between the plurality of hierarchical certifying tier, that certify the digital signature. In addition see col. 6, lines 32-38 "A second verify that the signer's signature is authentic. The verifier may acquire

Art Unit: 2134

the signer's public key certificate directly from the signer or indirectly from, e.g., a public registry".

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,867,578 by Brickell et al. (hereinafter '578).

As to independent claim 1, "A method for encrypting a message to be transmitted over a network, wherein the method comprises the steps of:" is taught in '578 col. 7, line 34 through 'col. 8, line 14;

"encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; and transmitting the encrypted message through the network to a recipient, wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network" is taught in '578 col. 6, line 57 through col. 7, line 15.

As to dependent claim 2, "wherein the encrypted message is generated by first selecting a random element  $k$  from an interval  $[0 \dots q-1]$ , where  $q$  denotes the size of a group  $G$ , using modulo  $p$ , then computing a symmetric key  $K = \text{hash}(g^k \text{ mod } p)$

Art Unit: 2134

p) for a symmetric encryption technique (E,D), where  $g$  is a generator of the group  $G$ , and finally computing the encrypted message in the form of a ciphertext  $M' = E_K(M)$ , where  $M$  denotes the message being encrypted” is shown in ‘578 col. 9, line 10 through col. 10, line 40.

As to dependent claim 3, “wherein also associated with the encrypted message is an element  $a = y_d^I * g^k$  and an element  $b = g^I$ , where  $I$  is chosen uniformly at random from  $[0 \dots q-1]$  and  $y_d$  is a public encryption key” is disclosed in ‘578 col. 9, lines 10-45.

As to dependent claim 4, “wherein the proof of correctness comprises a proof of knowledge of  $(I,k)$  that does not  $y_d^I$  or  $g^k$ ” is taught in ‘578 col. 7, lines 1-5.

As to dependent claim 5, “wherein also associated with the encrypted message is a certificate  $C_d$  on a public encryption key  $y_d$ ” is shown in ‘578 col. 10, lines 15-19.

As to dependent claim 6, “wherein the encrypted message is considered valid by the module of the server if the proof of correctness is valid and the certificate  $C_d$  is valid” is disclosed in ‘578 col. 10, lines 26-31.

As to dependent claim 7, “wherein the certificate  $C_d$  is considered valid if it is a valid certificate for encryption” is taught in ‘578 col. 10, lines 26-31.

As to dependent claim 8, “wherein the proof of correctness comprises a proof  $c$  in the form of a triple  $(r, s1, s2)$ ” is taught in ‘578 col. 17, lines 33-38.

As to dependent claim 9, “wherein the proof  $c$  is generated using the steps of: selecting two elements  $\mathfrak{g}_1$  and  $\mathfrak{g}_2$  at random from an interval  $[0 \dots q-1]$ ; computing  $r = y_d^{\mathfrak{g}_2} g^{\mathfrak{g}_2} \pmod{p}$ ; computing  $e = \text{hash}(r, a)$ ; computing  $s1 = \mathfrak{g}_1 + e * I \pmod{q}$ ;

Art Unit: 2134

computing  $s_2 = g^2 + e * k \pmod{q}$  and outputting the triple  $(r, s_1, s_2)$  as the proof  $c$ ” is taught in ‘578

col. 21, line 66 through col. 22, line 65.

As to dependent claim 10, “wherein the encrypted message is decrypted by a recipient using the steps of: computing  $B = b^{x_d} \pmod{p}$ , where  $x_d$  is a secret key corresponding to a public key  $y_d$ ; computing  $K = \text{hash}(I/B \pmod{p})$ ; and computing the message  $M$  as  $M = D_K(M')$ ” is taught in ‘578 col. 9, line 10 through col. 10, line 40.

As to dependent claim 11, “wherein the proof of correctness comprising the proof  $c$  in the form of the triple  $(r, s_1, s_2)$  is checked by computing  $e = \text{hash}(r, a)$  and verifying that  $y_d^{s_1} * g^{s_2} = r * a^e$ ” is shown in ‘578 col. 21, line 66 through col. 22, line 65.

As to dependent claim 12, “wherein if the check of the proof of correctness indicates that the proof is invalid, the module of the server directs that the encrypted message be discarded” is disclosed in ‘578 col. 7, lines 25-34.

As to dependent claim 13, “wherein the network comprises a plurality of servers, and wherein each of at least a subset of the servers includes a module for checking the proof of correctness if the corresponding encrypted message passes through the corresponding server in being transmitted from a sender to the recipient through the network” is taught in ‘578 col. 7, line 34 through col. 8, line 47.

As to dependent claim 14, “wherein the one or more escrow authorities comprises an escrow authority associated with a public key used for encryption of the message, and wherein the escrow authority associated with the public key is able to decrypt the encrypted message to obtain a plaintext message” is shown in ‘578 col. 6, lines 16-65.

As to dependent claim 15, “wherein the escrow agent associated with the public key is able to decrypt the encrypted message without exposing a corresponding secret key, using a threshold-based method” is disclosed in ‘578 col. 10, lines 52-67.

As to dependent claim 16, “wherein associated with the encrypted message is a first element that is generated using a public key of the recipient and can be decrypted by a party holding the corresponding secret key, and a second element that proves that the first element can be decrypted by a party holding the corresponding secret key” is taught in ‘578 col. 6, lines 57-65

As to independent claim 17, this claim is directed to an apparatus of the method of claim 1 and it is rejected along the same rationale.

As to independent claim 18, this claim is directed to an article of manufacture comprising one or more software programs of the method of claim 1 and it is rejected along the same rationale.

### **Conclusion**

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the

Art Unit: 2134

statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran  
Patent Examiner  
Technology Center 2134  
12 April 2005

  
**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**